

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-320403

(43)Date of publication of application : 16.11.2001

(51)Int.Cl.

H04L 12/54

H04L 12/58

G06F 13/00

H04L 9/14

(21)Application number : 2000-138118

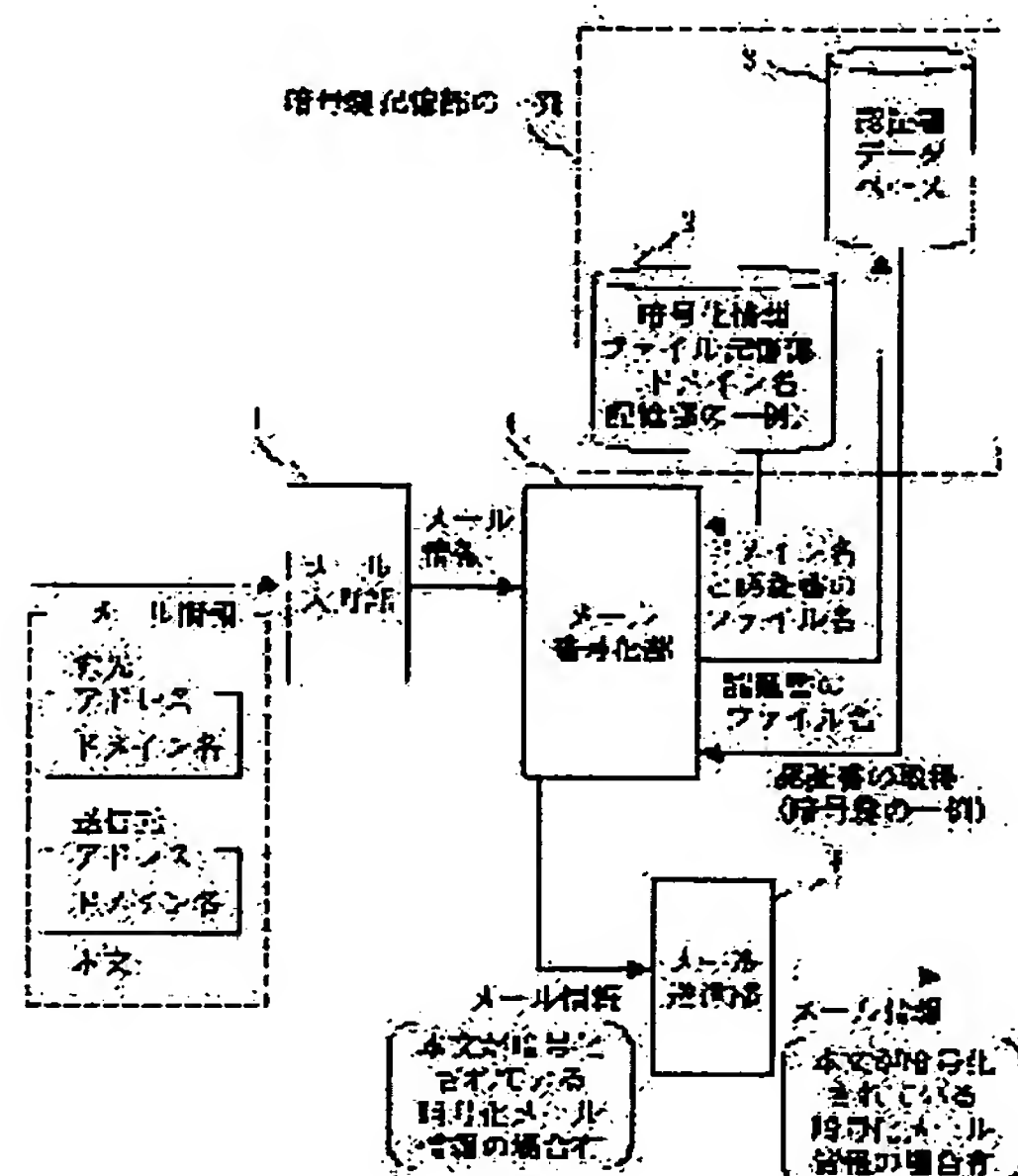
(71)Applicant : MITSUBISHI ELECTRIC  
SYSTEMWARE CORP

(22)Date of filing : 11.05.2000

(72)Inventor : HIRAI NOBUNAGA

(54) MAIL TRANSMITTER, MAIL RECEIVER, MAIL TRANSMISSION METHOD, MAIL  
RECEPTION METHOD AND COMPUTER-READABLE RECORDING MEDIUM WITH RECORDED  
PROGRAM TO ALLOW COMPUTER TO EXECUTE IT

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an electronic  
mail from being intercepted and falsified without the  
need for encrypting/decoding by each client computer.SOLUTION: A server receives mail information  
transmitted from clients and acquires a domain name  
from a destination address of the mail information. The  
server retrieves a domain name matched with the  
acquired domain name from an encryption information  
file. As a result of the retrieval, when there is any  
domain name matched with the acquired domain name,  
the server conducts encryption.

## LEGAL STATUS

[Date of request for examination] 21.09.2001

[Date of sending the examiner's decision of  
rejection] 01.06.2004[Kind of final disposal of application other than  
the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-320403

(P2001-320403A)

(43)公開日 平成13年11月16日(2001. 11. 16)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 12/54		G 0 6 F 13/00	6 1 0 S 5 J 1 0 4
12/58		H 0 4 L 11/20	1 0 1 B 5 K 0 3 0
G 0 6 F 13/00	6 1 0	9/00	6 4 1
H 0 4 L 9/14			

審査請求 未請求 請求項の数20 O L (全 15 頁)

(21)出願番号 特願2000-138118(P2000-138118)

(22)出願日 平成12年5月11日(2000. 5. 11)

(71)出願人 394013002

三菱電機システムウェア株式会社

神奈川県横浜市戸塚区川上町87番地1

(72)発明者 平井 延長

神奈川県横浜市戸塚区川上町87番地1 三

菱電機システムウェア株式会社内

(74)代理人 100099461

弁理士 溝井 章司

Fターム(参考) 5J104 AA01 AA09 AA33 AA35 DA03

JA21 LA06 NA02 PA08

5K030 GA15 GA17 HA06 HC01 JT02

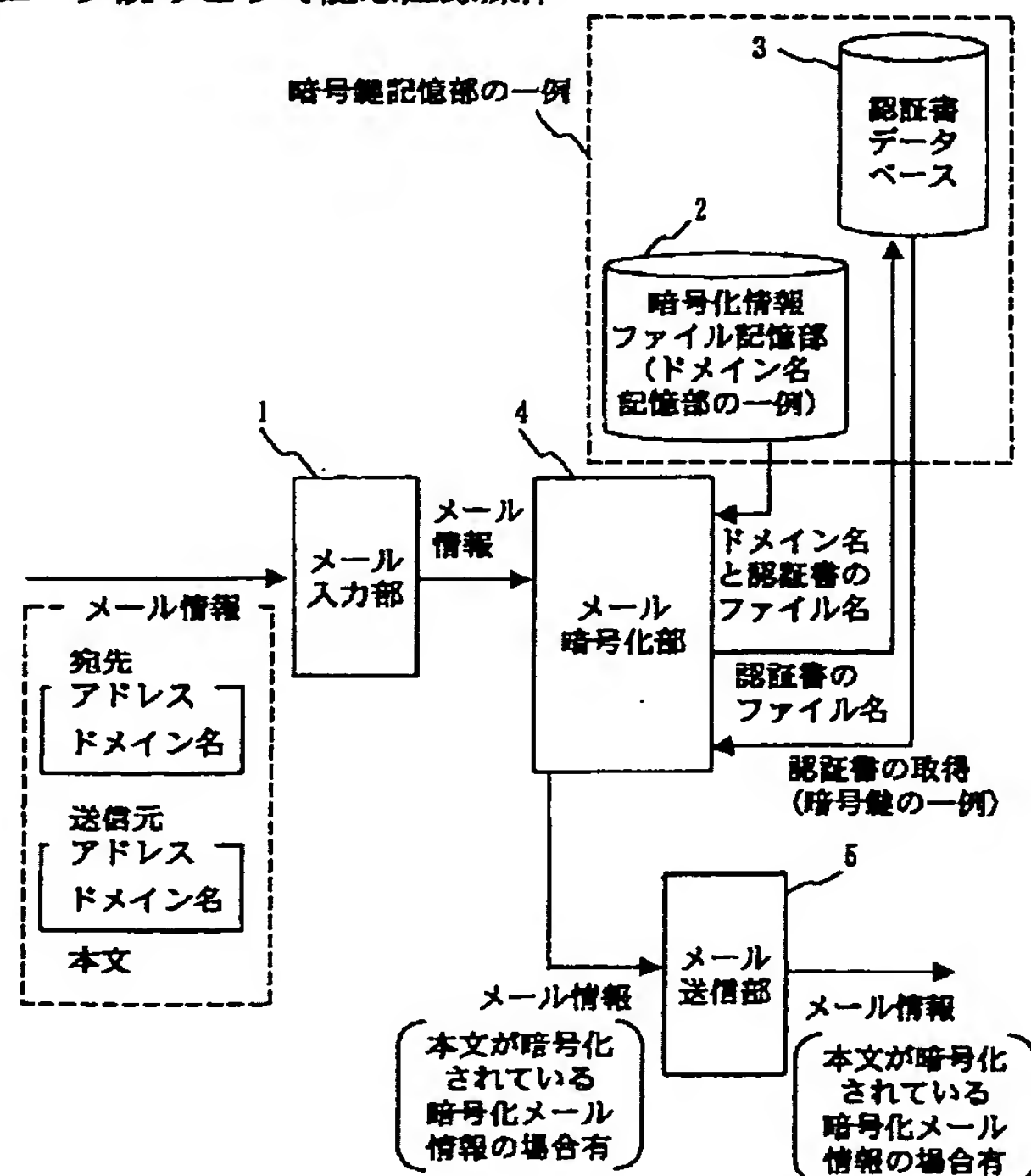
LD19

(54)【発明の名称】 メール送信装置、メール受信装置、メール送信方法、メール受信方法及びコンピュータに実行させるためのプログラムを記録したコンピュータ読みとり可能な記録媒体

(57)【要約】

【課題】 クライアントコンピュータごとに暗号化／復号をせずに電子メールの盗聴や改竄を防止する。

【解決手段】 サーバがクライアントより送信されてくるメール情報を入力して、メール情報の宛先アドレスよりドメイン名を取得する。取得したドメイン名と一致するドメイン名を暗号化情報ファイルの中から検索する。検索した結果、一致するドメイン名がある場合、暗号化を行う。



## 【特許請求の範囲】

【請求項 1】 以下の要素を有することを特徴とするメール送信装置

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力部、(2) 暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール入力部により入力されたメール情報に含まれる本文を暗号化するメール暗号化部、(4) メール入力部により入力されたメール情報に含まれる宛先アドレスと、メール暗号化部により暗号化された本文とを含む暗号化メール情報を送信するメール送信部。

【請求項 2】 メール送信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて暗号鍵を記憶する暗号鍵記憶部を有し、

メール暗号化部は、ドメイン名記憶部に記憶しているドメイン名であって、メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている暗号鍵を用いて、本文を暗号化することを特徴とする請求項 1 記載のメール送信装置。

【請求項 3】 メール送信装置は、ネットワークを介してクライアントと接続するサーバであって、メール入力部は、クライアントからネットワークを介してメール情報を入力することを特徴とする請求項 1 記載のメール送信装置。

【請求項 4】 以下の要素を有することを特徴とするメール受信装置

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信部、(2) 復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール受信部により受信されたメール情報は、本文が暗号化されている暗号化メール情報であると判断し、暗号化されている本文を復号するメール復号部。

【請求項 5】 メール受信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて復号鍵を記憶する復号鍵記憶部を有し、

メール復号部は、ドメイン名記憶部に記憶しているドメイン名であって、メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている復号鍵を用いて、本文を復号することを特徴とする請求項 4 記載のメール受信装置。

【請求項 6】 メール受信装置は、ネットワークを介し

てクライアントと接続するサーバであって、

更に、メール受信部により受信されたメール情報に含まれる送信元アドレスと、メール復号部により復号された本文とを含む復号メール情報を、ネットワークを介してクライアントへ出力するメール出力部を有することを特徴とする請求項 4 記載のメール受信装置。

【請求項 7】 以下の要素を有することを特徴とするメール送信装置

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力部、(2) 電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール入力部により入力されたメール情報に電子署名する電子署名部、(4) 電子署名部で電子署名したメール情報を送信するメール送信部。

【請求項 8】 メール送信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて暗号鍵を記憶する暗号鍵記憶部を有し、

電子署名部は、ドメイン名記憶部に記憶しているドメイン名であって、メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている暗号鍵を用いて、メール情報に電子署名することを特徴とする請求項 7 記載のメール送信装置。

【請求項 9】 メール送信装置は、ネットワークを介してクライアントと接続するサーバであって、メール入力部は、クライアントからネットワークを介してメール情報を入力することを特徴とする請求項 7 記載のメール送信装置。

【請求項 10】 以下の要素を有することを特徴とするメール受信装置

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信部、(2) 署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール受信部により受信されたメール情報の電子署名を署名検証する署名検証部。

【請求項 11】 メール受信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて認証書を記憶する認証書記憶部を有し、

署名検証部は、ドメイン名記憶部に記憶しているドメイン名であって、メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている認証書を用いて、メール情報の電子署名を署名検証することを特徴とする請求項 10 記載のメール受信装置。

【請求項 12】 メール受信装置は、ネットワークを介してクライアントと接続するサーバであって、更に、署名検証部により署名検証したメール情報を、ネットワークを介してクライアントへ出力するメール出力部を有することを特徴とする請求項 10 記載のメール受信装置。

【請求項 13】 以下の要素を有することを特徴とするメール送信方法

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力工程、(2) 暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール入力工程により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール入力工程により入力されたメール情報に含まれる本文を暗号化するメール暗号化工程、(4) メール入力工程により入力されたメール情報に含まれる宛先アドレスと、メール暗号化工程により暗号化された本文とを含む暗号化メール情報を送信するメール送信工程。

【請求項 14】 以下の要素を有することを特徴とするメール受信方法

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信工程、(2) 復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール受信工程により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール受信工程により受信されたメール情報は、本文が暗号化されている暗号化メール情報であると判断し、暗号化されている本文を復号するメール復号工程。

【請求項 15】 以下の要素を有することを特徴とするメール送信方法

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力工程、(2) 電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール入力工程により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール入力工程により入力されたメール情報に電子署名する電子署名工程、(4) 電子署名工程で電子署名したメール情報を送信するメール送信工程。

【請求項 16】 以下の要素を有することを特徴とするメール受信方法

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信工程、(2) 署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール受信工程により受信

されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール受信工程により受信されたメール情報の電子署名を署名検証する署名検証工程。

【請求項 17】 メール送信装置であるコンピュータに、以下の処理を実行させるためのプログラムを記録したコンピュータ読みとり可能な記録媒体

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力処理、(2) 暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール入力処理により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール入力処理により入力されたメール情報に含まれる本文を暗号化するメール暗号化処理、(4) メール入力処理により入力されたメール情報に含まれる宛先アドレスと、メール暗号化処理により暗号化された本文とを含む暗号化メール情報を送信するメール送信処理。

【請求項 18】 メール受信装置であるコンピュータに、以下の処理を実行させるためのプログラムを記録したコンピュータ読みとり可能な記録媒体

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信処理、(2) 復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール受信処理により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール受信処理により受信されたメール情報は、本文が暗号化されている暗号化メール情報であると判断し、暗号化されている本文を復号するメール復号処理。

【請求項 19】 メール送信装置であるコンピュータに、以下の処理を実行させるためのプログラムを記録したコンピュータ読みとり可能な記録媒体

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力処理、(2) 電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール入力処理により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール入力処理により入力されたメール情報に電子署名する電子署名処理、(4) 電子署名処理で電子署名したメール情報を送信するメール送信処理。

【請求項 20】 メール受信装置であるコンピュータに、以下の処理を実行させるためのプログラムを記録したコンピュータ読みとり可能な記録媒体

(1) ドメイン名を含む送信元アドレスと、本文とを含む

むメール情報を受信するメール受信処理、(2)署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3)メール受信処理により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール受信処理により受信されたメール情報の電子署名を署名検証する署名検証処理。

#### 【発明の詳細な説明】

#### 【0001】

【発明の属する技術分野】本発明は、電子メール（以下、メールという。）を送信するメール送信装置及びメール受信装置に関し、特に、クライアントコンピュータで意識せずメールの盗聴や改竄を防ぐことができるメール送信装置及びメール受信装置に関する。

#### 【0002】

【従来の技術】従来の技術を図16を用いて説明する。図16は、A社とB社との間でメールの送受信を行う場合を示す簡単な構成図である。図16において、100は、A社のメールサーバを示しており、101、102は、それぞれA社サーバ100のクライアントコンピュータを示している。また、200は、B社のメールサーバを示しており、201、202は、それぞれB社サーバ200のクライアントコンピュータを示している。なお、太い矢印線は、メールが暗号化された状態で送信されていることを示している。細い矢印線は、メールが暗号化されていない状態を示している。

【0003】各クライアントコンピュータには、それぞれ秘密鍵とそれに対応した公開鍵を含む証明書がユーザ単位で設定されているとともに、暗号化や復号するためのアプリケーションソフトウェアがインストールされている。

【0004】このような状況下、ユーザAのクライアントコンピュータ101よりメールを送信し、ユーザDのクライアントコンピュータ202がこのメールを受信する場合を説明する。

【0005】クライアントコンピュータ101は、ユーザDの公開鍵を含む証明書を取得し、証明書に含まれるユーザDの公開鍵を使用してメールを暗号化する。暗号化されたメールは、A社のメールサーバ100に送信され、A社のメールサーバ100によりB社のメールサーバ200に送信される。B社のメールサーバ200に送信されたメールは、ユーザDのクライアントコンピュータ202に送信され、ユーザD自身の秘密鍵を用いて復号される。

【0006】このように従来は、各ユーザのクライアントコンピュータがメールの暗号化や復号を行うことによりメールの盗聴を防止していた。

【0007】しかし、上述した方法では、ユーザのクライアントコンピュータごとに鍵や証明書の管理、暗号化

や復号の設定作業をしなければならず煩雑であるという問題点があった。ここで、暗号化する宛先アドレスを予め記憶しておき、送信しようとするメールの宛先アドレスと予め記憶しておいた暗号化する宛先アドレスが一致する場合にメールを暗号化することも考えられる。図16を例にとると、A社メールサーバ100のクライアントコンピュータ101がB社メールサーバ200のクライアントコンピュータ201のメールアドレス「userC@BBB.co.jp」、とクライアントコンピュータ202のメールアドレス「userD@BBB.co.jp」を暗号化する宛先アドレスとして記憶し、送信しようとするメールの宛先アドレスが記憶したメールアドレスと一致する場合に暗号化することもできる。

【0008】しかし、例えば、B社メールサーバ200にメールアドレス「userE@BBB.co.jp」を有するクライアントコンピュータ203が追加されたとすると、そのメールアドレスを暗号化する宛先アドレスとして設定する必要がある。しかし、設定は、人が行うので設定もれを起こす場合がある。この場合、メールが暗号化されず、企業の秘密情報が漏れてしまうという問題点があった。

【0009】また、ユーザのクライアントコンピュータごとに暗号化や復号をするためのアプリケーションソフトウェアをインストールしなければならず、導入や保守にかかる費用が高くなるという問題点があった。

【0010】さらに、ユーザのクライアントコンピュータで暗号化を行っていたため、例えば、A社のメールサーバ管理者が重要な機密情報の社外流出をチェックすることができないという問題点があった。

#### 【0011】

【発明が解決しようとする課題】本発明は上記した従来技術の問題点を除くためになされたものであって、その目的は、ユーザのクライアントコンピュータごとに暗号化や復号をせずにメールの盗聴や改竄を防止できるようにすることにある。また、クライアントコンピュータのメールアドレスが追加、変更されても、設定作業をしないで済み、設定もれをなくすことにある。

【0012】また、他の目的は、企業内の機密情報流出をチェックできるようにすることにある。

#### 【0013】

【課題を解決するための手段】本発明に係るメール送信装置は、以下の要素を備えることを特徴とする。

(1)ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力部、(2)暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3)メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール入力部により入力されたメール情報に含まれる本文を暗号化するメール暗号化部、(4)

メール入力部により入力されたメール情報に含まれる宛先アドレスと、メール暗号化部により暗号化された本文とを含む暗号化メール情報を送信するメール送信部。

【0014】また、本発明に係るメール送信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて暗号鍵を記憶する暗号鍵記憶部を有し、メール暗号化部は、ドメイン名記憶部に記憶しているドメイン名であって、メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている暗号鍵を用いて、本文を暗号化することを特徴とする。

【0015】また、本発明に係るメール送信装置は、ネットワークを介してクライアントと接続するサーバであって、メール入力部は、クライアントからネットワークを介してメール情報を入力することを特徴とする。

【0016】本発明に係るメール受信装置は、以下の要素を備えることを特徴とする。

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信部、(2) 復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール受信部により受信されたメール情報は、本文が暗号化されている暗号化メール情報であると判断し、暗号化されている本文を復号するメール復号部。

【0017】また、本発明に係るメール受信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて復号鍵を記憶する復号鍵記憶部を有し、メール復号部は、ドメイン名記憶部に記憶しているドメイン名であって、メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている復号鍵を用いて、本文を復号することを特徴とする。

【0018】また、本発明に係るメール受信装置は、ネットワークを介してクライアントと接続するサーバであって、更に、メール受信部により受信されたメール情報に含まれる送信元アドレスと、メール復号部により復号された本文とを含む復号メール情報を、ネットワークを介してクライアントへ出力するメール出力部を有することを特徴とする。

【0019】本発明に係るメール送信装置は、以下の要素を備えることを特徴とする。

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力部、(2) 電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一

致する場合に、メール入力部により入力されたメール情報に電子署名する電子署名部、(4) 電子署名部で電子署名したメール情報を送信するメール送信部。

【0020】また、メール送信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて暗号鍵を記憶する暗号鍵記憶部を有し、電子署名部は、ドメイン名記憶部に記憶しているドメイン名であって、メール入力部により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている暗号鍵を用いて、メール情報に電子署名することを特徴とする。

【0021】また、本発明に係るメール送信装置は、ネットワークを介してクライアントと接続するサーバであって、メール入力部は、クライアントからネットワークを介してメール情報を入力することを特徴とする。

【0022】本発明に係るメール受信装置は、以下の要素を備えることを特徴とする。

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信部、(2) 署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部、(3) メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶部に記憶しているドメイン名とが一致する場合に、メール受信部により受信されたメール情報の電子署名を署名検証する署名検証部。

【0023】また、本発明に係るメール受信装置は、ドメイン名記憶部に記憶しているドメイン名に対応付けて認証書を記憶する認証書記憶部を有し、署名検証部は、ドメイン名記憶部に記憶しているドメイン名であって、メール受信部により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と一致するドメイン名に対応付けられている認証書を用いて、メール情報の電子署名を署名検証することを特徴とする。

【0024】また、本発明に係るメール受信装置は、ネットワークを介してクライアントと接続するサーバであって、更に、署名検証部により署名検証したメール情報を、ネットワークを介してクライアントへ出力するメール出力部を有することを特徴とする。

【0025】本発明に係るメール送信方法は、以下の工程を備えることを特徴とする。

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力工程、(2) 暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール入力工程により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール入力工程により入力されたメール情報に含まれる本文を暗号化するメール暗号化工程、(4) メール入力工程により入力されたメール情報に含まれる宛先アドレスと、メール暗号化工程により

暗号化された本文とを含む暗号化メール情報を送信するメール送信工程。

【0026】本発明に係るメール受信方法は、以下の工程を備えることを特徴とする。

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信工程、(2) 復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール受信工程により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール受信工程により受信されたメール情報は、本文が暗号化されている暗号化メール情報であると判断し、暗号化されている本文を復号するメール復号工程。

【0027】本発明に係るメール送信方法は、以下の工程を備えることを特徴とする。

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力工程、(2) 電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール入力工程により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール入力工程により入力されたメール情報に電子署名する電子署名工程、(4) 電子署名工程で電子署名したメール情報を送信するメール送信工程。

【0028】本発明に係るメール受信方法は、以下の工程を備えることを特徴とする。

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信工程、(2) 署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶工程、(3) メール受信工程により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶工程により記憶されたドメイン名とが一致する場合に、メール受信工程により受信されたメール情報の電子署名を署名検証する署名検証工程。

【0029】プログラムを記録したコンピュータ読みとり可能な記録媒体は、メール送信装置であるコンピュータに、以下の処理を実行させることを特徴とする。

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力処理、(2) 暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール入力処理により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール入力処理により入力されたメール情報に含まれる本文を暗号化するメール暗号化処理、(4) メール入力処理により入力されたメール情報に含まれる宛先アドレスと、メール暗号化処理により

暗号化された本文とを含む暗号化メール情報を送信するメール送信処理。

【0030】プログラムを記録したコンピュータ読みとり可能な記録媒体は、メール受信装置であるコンピュータに以下の処理を実行させることを特徴とする。

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信処理、(2) 復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール受信処理により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール受信処理により受信されたメール情報は、本文が暗号化されている暗号化メール情報であると判断し、暗号化されている本文を復号するメール復号処理。

【0031】プログラムを記録したコンピュータ読みとり可能な記録媒体は、メール送信装置であるコンピュータに、以下の処理を実行させることを特徴とする。

(1) ドメイン名を含む宛先アドレスと、本文とを含むメール情報を入力するメール入力処理、(2) 電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール入力処理により入力されたメール情報に含まれる宛先アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール入力処理により入力されたメール情報に電子署名する電子署名処理、(4) 電子署名処理で電子署名したメール情報を送信するメール送信処理。

【0032】メール受信装置であるコンピュータに、以下の処理を実行させるためのプログラムを記録したコンピュータ読みとり可能な記録媒体。

(1) ドメイン名を含む送信元アドレスと、本文とを含むメール情報を受信するメール受信処理、(2) 署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶処理、(3) メール受信処理により受信されたメール情報に含まれる送信元アドレスに含まれるドメイン名と、ドメイン名記憶処理により記憶されたドメイン名とが一致する場合に、メール受信処理により受信されたメール情報の電子署名を署名検証する署名検証処理。

【0033】

【発明の実施の形態】図1は、A社、B社、C社の間でメールの送受信を行う場合を示す簡単な構成図である。図において、50、60、70は、それぞれA社、B社、C社のメールサーバを示しており、51、52は、A社メールサーバのクライアントコンピュータを示している。同様に、61、62は、B社メールサーバのクライアントコンピュータを示しており、71、72は、C社メールサーバのクライアントコンピュータを示している。

【0034】なお、太い矢印線は、暗号化されたメール、または電子署名されたメールが送受信されることを示しており、細い矢印線は、暗号化や電子署名がされていないメールが送受信されることを示している。したがって、メールサーバ50とメールサーバ60間のメールの送受信は、暗号化され、メールサーバ50とメールサーバ70間のメールの送受信は、暗号化されないことを示している。

【0035】以下に述べる実施の形態では、図1のメールサーバ50を本発明に係るメール送信装置の一例として説明し、図1のメールサーバ60を本発明に係るメール受信装置の一例として説明する。

【0036】実施の形態1. 実施の形態1では、クライアントより送信されてきたメールをドメイン名によって暗号化するメール送信装置について説明する。

【0037】図2は、実施の形態1に係るメール送信装置の機能構成図を示した図である。図において、メール送信装置は、メール入力部1、暗号化情報ファイル記憶部2、認証書データベース3、メール暗号化部4、メール送信部5より構成されている。

【0038】メール入力部1は、例えば、図1に示すクライアントコンピュータ51よりメール情報を入力し、入力したメール情報をメール暗号化部4に出力するように構成されており、SMTP(Simple Mail Transfer Protocol)の受信機能を用いる。メール入力部1により入力されるメール情報には、図2に示すように宛先アドレスと送信元アドレスと本文が含まれている。

【0039】暗号化情報ファイル記憶部2は、例えば図3に示す暗号化情報ファイル6を記憶するものであり、暗号化を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部の一例である。暗号化情報ファイル6は、例えば、暗号化を要するメール情報を特定するドメイン名と、認証書のファイル名を対応づけたファイルである。具体的に図3には、宛先アドレスのドメイン名「BBB.co.jp」に認証書のファイル名「certification BBB」が対応付けられている。例えば、B社メールサーバ60のドメイン名を「BBB.co.jp」とすると、A社メールサーバ50からB社メールサーバ60へ送信されるメールの宛先アドレスに含まれるドメイン名には、「BBB.co.jp」があるので、暗号化される。一方、C社メールサーバ70のドメイン名を「CCC.co.jp」とすると、A社メールサーバ50からC社メールサーバ70へ送信されるメールの宛先アドレスに含まれるドメイン名は、暗号化情報ファイル6にないので暗号化されない。なお、認証書を特定する暗号化情報として、認証書のファイル名でなく例えば、認証書の発行者名とシリアル番号にしてもよい。

【0040】認証書データベース3は、認証書(暗号鍵の一例)を記憶するように構成されている。この認証書

データベース3と暗号化情報ファイル記憶部2とを組み合わせたものが、ドメイン名に対応付けて認証書を記憶する暗号鍵記憶部の一例である。

【0041】メール暗号化部4は、メール入力部1よりメール情報を入力し、そのメール情報に含まれる宛先アドレスのドメイン名より、本文への暗号化を要するか判断し、暗号化を要すると判断した場合に本文の暗号化を行うように構成されている。そして、メール情報(本文を暗号化した暗号化メール情報を含む)をメール送信部5に出力するように構成されている。なお、暗号化には、S/MIME形式などを用いることができる。

【0042】メール送信部5は、メール暗号化部4よりメール情報(本文を暗号化した暗号化メール情報を含む)を入力し、図1に示すメールサーバ60やメールサーバ70に送信するように構成されており、SMTPの送信機能を利用する。

【0043】実施の形態1に係るメール送信装置は、上記のように構成されており、以下にその動作について図4を参照しながら説明する。

【0044】予め、暗号化を要するメール情報を特定するドメイン名と認証書のファイル名を対応付けた暗号化情報ファイル6は、暗号化情報ファイル記憶部2に記憶されており(ドメイン名記憶工程、図示せず)、また、認証書自体は、認証書データベース3に記憶されているものとする。

【0045】まず、例えば、図1に示すクライアント51よりメール情報を入力する(S11メール入力工程)。次に、入力したメール情報に含まれる宛先アドレスからドメイン名を取得し(S120)、その取得したドメイン名と一致するドメイン名を暗号化情報ファイル6の中から検索する(S121)。

【0046】暗号化情報ファイル6を検索した結果、一致するドメイン名があれば、本文を暗号化する必要があると判断し(S122)、そのドメイン名に対応付けられている認証書のファイル名より認証書を取得する(S123)。そして、取得した認証書に基づきメール情報の本文の暗号化を行い(S124)、本文を暗号化した暗号化メール情報を図1に示すメールサーバ60へ送信する(S13メール送信工程)。

【0047】暗号化情報ファイル6を検索した結果、一致するドメイン名が無ければ、本文を暗号化する必要がないと判断し(S125)、暗号化せずに、メール情報を図1に示すメールサーバ70へ送信する(S13メール送信工程)。

【0048】実施の形態2. 実施の形態2では、送信されてきたメールの送信元アドレスのドメイン名によって復号するメール受信装置について説明する。図1における、メールサーバ60に対応する。

【0049】図5は、実施の形態2に係るメール受信装置の機能構成図を示した図である。図において、メール

受信装置は、メール受信部 7、復号情報ファイル記憶部 8、秘密鍵記憶部 9、メール復号部 10、メール蓄積部 11、メール出力部 12 より構成されている。

【0050】メール受信部 7 は、例えば、図 1 に示すメールサーバ 50 やメールサーバ 70 よりメール情報を入力し、入力したメール情報をメール復号部 10 に出力するように構成されており、SMTP (Simple Mail Transfer Protocol) の受信機能を利用する。メール受信部 7 により入力されるメール情報には、図 5 に示すように宛先アドレスと送信元アドレスと本文が含まれている。また、本文が暗号化されている暗号化メール情報の場合もある。例えば、図 1 のメールサーバ 50 より受信する場合は、暗号化メール情報であり、メールサーバ 70 より受信する場合は、本文が暗号化されていないメール情報である。

【0051】復号情報ファイル記憶部 8 は、例えば図 6 に示す復号情報ファイル 6 を記憶するものであり、復号を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部の一例である。復号情報ファイル 13 は、例えば、復号を要するメール情報を特定するドメイン名と秘密鍵のファイル名を対応づけたファイルである。具体的に図 6 では、送信元アドレスのドメイン名「YYY.co.jp」、「SYZ.co.jp」などに秘密鍵のファイル名「secret1」が対応付けられている。なお、普通秘密鍵は 1 つであるが、例えば、秘密鍵を複数設定し、ドメイン名によって、異なる秘密鍵のファイル名を対応付けてもよい。

【0052】秘密鍵記憶部 9 は、秘密鍵（復号鍵の一例）を記憶するように構成されている。この秘密鍵記憶部 9 と復号情報ファイル記憶部 8 とを組み合わせたものが、ドメイン名に対応付けて秘密鍵を記憶する復号鍵記憶部の一例である。

【0053】メール復号部 10 は、メール受信部 7 よりメール情報（暗号化メール情報を含む）を入力し、そのメール情報に含まれる宛先アドレスのドメイン名より本文の復号を要するかどうかを判断し、復号を要すると判断した場合に本文の復号を行うように構成されている。そして、メール情報（本文を復号した復号メール情報を含む）をメール出力部 12 に出力するように構成されている。なお、復号には、S/MIME 形式などを用いることができる。

【0054】メール蓄積部 11 は、メール情報（本文を復号した復号メール情報を含む）を蓄積するものであり、例えば SMTP の蓄積機能を用いて、メール蓄積部 11 にメール情報が蓄積される。

【0055】メール出力部 12 は、メール復号部 10 よりメール情報（本文を暗号化した暗号化メール情報を含む）を入力し、例えば、図 1 に示すクライアント 61 やクライアント 62 の要求によりメール情報を出力するように構成されており、POP (Post Office

Protocol) 応答機能や IMAP4 (Internet Message Access Protocol version 4) 応答機能を利用する。

【0056】実施の形態 2 に係るメール受信装置は、上記のように構成されており、以下にその動作について図 7 を参照しながら説明する。

【0057】予め、復号を要するメール情報を特定するドメイン名と秘密鍵のファイル名を対応付けた復号情報ファイル 13 は、復号情報ファイル記憶部 8 に記憶されており（ドメイン名記憶工程、図示せず）、また、秘密鍵自体は、秘密鍵記憶部に記憶されているものとする。なお、メール受信装置に入力されるメール情報には、本文が暗号化されている暗号化メール情報も含まれるが、入力した時点においては判断がつかないため、すべてのメール情報を同様に扱う。

【0058】まず、図 1 に示すメールサーバ 50 やメールサーバ 70 よりメール情報を受信する（S21 メール受信工程）。次に、受信したメール情報に含まれる送信元アドレスからドメイン名を取得し（S220）、その取得したドメイン名と一致するドメイン名を復号情報ファイル 13の中から検索する（S221）。

【0059】復号情報ファイル 13 を検索した結果、一致するドメイン名があれば、本文を復号する必要があると判断し（S222）、そのドメイン名に対応付けられている秘密鍵のファイル名より秘密鍵を取得する（S223）。そして、取得した秘密鍵に基づきメール情報の本文の復号を行い（S224）本文を復号した復号メール情報をメール蓄積部 11 に蓄積する（S23）。蓄積された復号メール情報は、例えば、図 1 に示すクライアント 61 やクライアント 62 より出力要求があると出力される（S24 メール出力工程）。

【0060】復号情報ファイル 13 を検索した結果、一致するドメイン名が無ければ、本文を復号する必要があると判断し（S225）、復号せずに、メール情報をメール蓄積部 11 に蓄積する（S23）。蓄積された復号メール情報は、例えば、図 1 に示すクライアント 61 やクライアント 62 より出力要求があると（S24）、出力される（S25 メール出力工程）。

【0061】実施の形態 3. 実施の形態 2 では、メール受信部 7 により受信したメール情報は、メール復号部 10 に入力され、メール情報に含まれる送信元アドレスのドメイン名より本文の復号を要するかどうかを判断し、復号を要すると判断した場合に本文の復号を行うように構成されている例を示した。この実施の形態 3 では、メール受信部 7 により受信したメール情報を、まずメール蓄積部 11 に蓄積し、クライアントより出力要求があるとメール復号部 10 において、復号を要するメール情報であるかを判断をする場合について説明する。

【0062】図 8 に、実施の形態 3 に係るメール受信装置の機能構成図を示す。図 8 は、図 5 とほぼ同じ構成を

している。相違する点は、メール受信部 7 が、受信したメール情報（暗号化メール情報を含む）をメール蓄積部 11 に出力する点と、メール復号部 10 がメール蓄積部 11 よりメール情報（暗号化メール情報を含む）を入力する点である。

【0063】次に、動作について図 9 を参照しながら説明する。予め、復号を要するメール情報を特定するドメイン名と秘密鍵のファイル名を対応付けた復号情報ファイル 13 は、復号情報ファイル記憶部に記憶されており（ドメイン名記憶工程、図示せず）、また、秘密鍵自体は、秘密鍵記憶部 9 に記憶されているものとする。なお、メール受信装置に入力されるメール情報には、本文が暗号化されている暗号化メール情報も含まれるが、入力した時点においては判断がつかないため、すべてのメール情報を同様に扱う。

【0064】まず、図 1 に示すメールサーバ 50 やメールサーバ 70 よりメール情報を受信し（S31 メール受信工程）、受信したメール情報は、メール蓄積部 11 に蓄積される（S32）。次に、例えば、図 1 に示すクライアント 61 やクライアント 62 より出力要求があると（S33）、メール復号部 10 は、メール蓄積部 11 よりメール情報を入力し、メール情報に含まれる送信元アドレスよりドメイン名を取得する（S341）。そして、その取得したドメイン名と一致するドメイン名を復号情報ファイル 13の中から検索する（S342）。

【0065】復号情報ファイル 13 を検索した結果、一致するドメイン名があれば、本文を復号する必要があると判断し（S343）、そのドメイン名に対応付けられている秘密鍵のファイル名より秘密鍵を取得する（S344）。そして、取得した秘密鍵に基づきメール情報の本文の復号を行い（S345）、本文を復号した復号メール情報をクライアントに出力する（S35 メール出力工程）。

【0066】復号情報ファイル 13 を検索した結果、一致するドメイン名が無ければ、本文を復号する必要がないと判断し（S346）、復号せずに、メール情報をクライアントに出力する。

【0067】このように実施の形態 3 に係るメール受信装置によれば、クライアントより出力要求があつてはじめて暗号化メール情報を復号するため、それまで暗号化メール情報は、本文が暗号化された状態でメール蓄積部 11 に蓄積されている。したがって、メール蓄積部 11 に不正にアクセスされても暗号化メール情報の場合、本文が暗号化されているため内容を知られないで済む。

【0068】なお、実施の形態 1、2、3 では、公開鍵暗号方式を使った暗号化／復号方式を使って説明したが共通鍵を使う共通鍵方式を用いてもよい。また、公開鍵暗号方式と共通鍵方式を組み合わせ用いてもよい。

【0069】実施の形態 4. 実施の形態 4 では、クライアントより送信されてきたメールをドメイン名によって

電子署名するメール送信装置について説明する。

【0070】図 10 は、実施の形態 4 に係るメール送信装置の機能構成図を示した図である。図において、メール送信装置は、メール入力部 1、電子署名情報ファイル記憶部 14、秘密鍵記憶部 15、電子署名部 16、メール送信部 4 より構成されている。

【0071】メール入力部 1 は、例えば、図 1 に示すクライアントコンピュータ 51 よりメール情報を入力し、入力したメール情報を電子署名部 16 に出力するように構成されている。

【0072】電子署名情報ファイル記憶部 14 は、例えば図 11 に示す電子署名情報ファイル 17 を記憶するものであり、電子署名を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部の一例である。電子署名情報ファイル 17 は、例えば、電子署名を要するメール情報を特定するドメイン名と秘密鍵のファイル名を対応づけたファイルである。具体的に図 11 には、宛先アドレスのドメイン名「ZZZ.co.jp」などに秘密鍵のファイル名「secret 2」が対応付けられている。なお、普通秘密鍵は 1 つであるが例えば、秘密鍵を複数設定し、ドメイン名によって、異なる秘密鍵のファイル名を対応付けてもよい。

【0073】秘密鍵記憶部 15 は、秘密鍵を記憶するように構成されている。この秘密鍵記憶部 15 と電子署名情報ファイル記憶部 14 とを組み合わせたものが、ドメイン名に対応付けて秘密鍵を記憶する暗号鍵記憶部の一例である。

【0074】電子署名部 16 は、メール入力部 1 よりメール情報を入力し、そのメール情報に含まれる宛先アドレスのドメイン名よりメール情報に電子署名を要するのかが判断し、電子署名を要すると判断した場合にメール情報に電子署名をするように構成されている。そして、メール情報（電子署名をしたメール情報を含む）をメール送信部 4 に出力するように構成されている。なお、電子署名には、S/MIME 形式などを用いることができる。

【0075】メール送信部 4 は、電子署名部 16 よりメール情報（電子署名したメール情報を含む）を入力し、図 1 に示すメールサーバ 60 やメールサーバ 70 に送信するように構成されている。

【0076】実施の形態 4 に係るメール送信装置は、上記のように構成されており、以下にその動作について図 12 を参照しながら説明する。

【0077】予め、電子署名を要するメール情報を特定するドメイン名と秘密鍵のファイル名を対応付けた電子署名情報ファイル 17 は、電子署名情報ファイル記憶部 14 に記憶されており（ドメイン名記憶工程、図示せず）、また、秘密鍵自体は、秘密鍵記憶部 15 に記憶されているものとする。

【0078】まず、例えば、図 1 に示すクライアント 5

1よりメール情報を入力する（S41メール入力工程）。次に、入力したメール情報に含まれる宛先アドレスからドメイン名を取得し（S420）、その取得したドメイン名と一致するドメイン名を電子署名情報ファイル17の中から検索する（S421）。

【0079】電子署名情報ファイル17を検索した結果、一致するドメイン名があれば、メール情報に電子署名する必要があると判断し（S422）、そのドメイン名に対応付けられている秘密鍵のファイル名より秘密鍵を取得する（S423）。そして、取得した秘密鍵に基づきメール情報に電子署名し（S424）、電子署名をしたメール情報を例えば、図1に示すメールサーバ60へ送信する（S43メール送信工程）。

【0080】電子署名情報ファイル17を検索した結果、一致するドメイン名が無ければ、電子署名する必要があると判断し（S425）、電子署名せずに、メール情報を図1に示すメールサーバ70へ送信する（S43メール送信工程）。

【0081】実施の形態5. 実施の形態5では、送信されてきたメールの送信元アドレスのドメイン名によって、電子署名したメール情報の署名検証をするメール受信装置について説明する。図1におけるメールサーバ60に対応する。

【0082】図13は、実施の形態5に係るメール受信装置の機能構成図を示した図である。図において、メール受信装置は、メール受信部7、署名検証情報ファイル記憶部18、認証書データベース19、署名検証部20、メール蓄積部11、メール出力部12より構成されている。

【0083】メール受信部7は、例えば、図1に示すメールサーバAやメールサーバCよりメール情報を入力し、入力したメール情報を署名検証部20に出力するように構成されている。

【0084】署名検証情報ファイル記憶部18は、例えば図14に示す署名検証情報ファイル21を記憶するものであり、署名検証を要するメール情報を特定するドメイン名を記憶するドメイン名記憶部の一例である。署名検証情報ファイル18は、例えば、署名検証を要するメール情報を特定するドメイン名と認証書のファイル名を対応づけたファイルである。具体的に図14には、送信元アドレスのドメイン名「XYZ.co.jp」に認証書のファイル名「sign XYZ」が対応付けられている。

【0085】認証書データベース19は、認証書を記憶するように構成されている。この認証書データベース19と署名検証情報ファイル記憶部18とを組み合わせたものが、ドメイン名に対応付けて認証書を記憶する認証書記憶部の一例である。

【0086】署名検証部20は、メール受信部7よりメール情報（電子署名をしたメール情報を含む）を入力し、そのメール情報に含まれる送信元アドレスのドメ

イン名より署名検証を要するのか判断し、署名検証を要すると判断した場合に電子署名したメール情報の署名検証をするように構成されている。そして、メール情報（電子署名を署名検証したメール情報を含む）をメール出力部12に出力するように構成されている。なお、署名検証には、S/MIME形式などを用いることができる。

【0087】メール蓄積部11は、メール情報（電子署名を署名検証したメール情報を含む）を蓄積するものであり、メール出力部12は、署名検証部20よりメール情報（電子署名の署名検証をしたメール情報を含む）を入力し、例えば、図1に示すクライアント61やクライアント62に出力するように構成されている。

【0088】実施の形態5に係るメール受信装置は、上記のように構成されており、以下にその動作について図15を参照しながら説明する。

【0089】予め、署名検証を要するメール情報を特定するドメイン名と認証書のファイル名を対応付けた署名検証情報ファイル21は、署名検証情報ファイル記憶部18に記憶されており（ドメイン名記憶工程、図示せず）、また、認証書自体は、認証書データベース19に記憶されているものとする。なお、メール受信装置に入力されるメール情報には、電子署名したメール情報も含まれるが、入力した時点においては判断がつかないため、すべてのメール情報を同様に扱う。

【0090】まず、図1に示すメールサーバ50やメールサーバ70よりメール情報を受信する（S51メール受信工程）。次に、受信したメール情報に含まれる送信元アドレスからドメイン名を取得し（S521）、その取得したドメイン名と一致するドメイン名を署名検証情報ファイル21の中から検索する（S522）。

【0091】署名検証情報ファイル21を検索した結果、一致するドメイン名があれば、電子署名されたメール情報として、署名検証する必要があると判断し（S523）、そのドメイン名に対応付けられている認証書のファイル名より認証書を取得する（S524）。そして、取得した認証書に基づき電子署名されたメール情報の署名検証を行い（S525）、署名検証したメール情報をメール蓄積部11に蓄積する（S53）。蓄積されたメール情報は、例えば、図1に示すクライアント61やクライアント62より出力要求があると（S54）出力される（S55メール出力工程）。

【0092】署名検証情報ファイル21を検索した結果、一致するドメイン名が無ければ、電子署名されていないメール情報であり、署名検証する必要があると判断する（S526）。そして、署名検証せずに、メール情報をメール蓄積部11に蓄積する（S53）。蓄積されたメール情報は、例えば、図1に示すクライアント61やクライアント62より出力要求があると（S54）、出力される（S55メール出力工程）。

【0093】実施の形態5では、メール受信部7により

受信したメール情報は、署名検証部 20 に入力され、メール情報に含まれる送信元アドレスのドメイン名より署名検証を要するのか判断する。そして、署名検証を要すると判断した場合に署名検証するように構成されている例を示した。しかし、メール受信部 7 により受信したメール情報を、まずメール蓄積部 11 に蓄積し、クライアントより出力要求があると署名検証部 20 において、署名検証を要するメール情報であるか判断をするように構成してもよい。

【0094】以上述べた実施の形態のメール送信装置は、暗号化のみ、電子署名のみ行う例を示したが、暗号化と電子署名の両方を行うように構成してもよい。同様にメール受信装置は、復号と署名検証の両方を行うように構成してもよい。

【0095】なお、暗号化／復号、電子署名／署名検証を S/MIME で行うことにより、暗号化／復号、電子署名／署名検証を行うメールサーバの多層化や暗号化／復号、電子署名／署名検証をクライアントで行ったメールについても処理できる。

【0096】

【発明の効果】本発明によれば、入力したメール情報の宛先アドレス自体ではなく、宛先アドレスに含まれるドメイン名を条件として暗号化を要するメール情報を特定するように構成したので、同じドメイン名を有する新たな宛先アドレスに対してメールを送信する場合でも、暗号化を要するメール情報を特定する条件の設定変更をする必要がない。つまり、同一ドメインに属する宛先アドレス群に対して一度設定を行えば、宛先アドレス毎に設定する必要がなくなる。したがって、設定もれによる企業の秘密情報の流出を防止することができる。また、設定作業の簡略化及びコストの削減を図ることができる効果を得られる。

【0097】本発明によれば、受信したメール情報の送信元アドレス自体ではなく、送信元アドレスに含まれるドメイン名を条件として復号を要するメール情報を特定するように構成したので、同じドメイン名を有する新たな送信元アドレスよりメールを受信した場合でも、復号を要するメール情報を特定する条件の設定変更をする必要がなく、自動的に復号することができる。つまり、同一ドメインに属する送信元アドレス群に対して一度設定を行えば、送信元アドレス毎に設定する必要がなくなる。また、設定作業の簡略化及びコストの削減を図ることができる効果を得られる。

【0098】本発明によれば、入力したメール情報の宛先アドレス自体ではなく、宛先アドレスに含まれるドメイン名を条件として電子署名を要するメール情報を特定するように構成したので、同じドメイン名を有する新たな宛先アドレスに対してメールを送信する場合でも、電子署名を要するメール情報を特定する条件の設定変更をする必要がなく、送信するメールへ自動的に電子署名さ

れる。つまり、同一ドメインに属する宛先アドレス群に対して一度設定を行えば、宛先アドレス毎に設定する必要がなくなる。また、設定作業の簡略化及びコストの削減を図ることができる効果を得られる。

【0099】本発明によれば、受信したメール情報の送信元アドレス自体ではなく、送信元アドレスに含まれるドメイン名を条件として署名検証を要するメール情報を特定するように構成したので、同じドメイン名を有する新たな送信元アドレスよりメールを受信した場合でも、署名検証を要するメール情報を特定する条件の設定変更をする必要がない。つまり、同一ドメインに属する送信元アドレス群に対して一度設定を行えば、送信元アドレス毎に設定する必要がなくなる。したがって、設定もれにより署名検証しなかったことで、メール情報の改竄を発見できないことを防止できる。また、設定作業の簡略化及びコストの削減を図ることができる効果を得られる。

【0100】また、ドメイン名は、企業単位で設定されることが多いが、本発明によれば、ドメイン名単位で、暗号化／復号又は電子署名／署名検証を要するメール情報を特定するように構成したので、企業単位でメール情報の暗号化／復号又は電子署名／署名検証をすることができる効果を得られる。すなわち、特定企業間のメールの暗号化／復号又は電子署名／署名検証を簡単に行うことができる。

【0101】また、本発明によれば、クライアントと接続するサーバでメール情報の暗号化／復号、電子署名／署名検証をするように構成したので、クライアントで意識せずメール情報の盗聴、改竄を防止できる効果を得られる。

【0102】また、本発明によれば、クライアントと接続するサーバでメール情報の暗号化／復号、電子署名／署名検証をするように構成したので、企業の機密情報の流出をサーバ管理者がチェックできる効果を得られる。

【図面の簡単な説明】

【図 1】 A 社、B 社、C 社の間でメールの送受信を行う場合を示す簡単な構成図である。

【図 2】 実施の形態 1 に係るメール送信装置の機能構成図を示す図である。

【図 3】 暗号化情報ファイルを示した図である。

【図 4】 実施の形態 1 に係るメール送信装置の動作を示したフローチャートである。

【図 5】 実施の形態 2 に係るメール受信装置の機能構成図を示す図である。

【図 6】 復号情報ファイルを示した図である。

【図 7】 実施の形態 2 に係るメール受信装置の動作を示したフローチャートである。

【図 8】 実施の形態 3 に係るメール受信装置の機能構成図を示す図である。

【図 9】 実施の形態 3 に係るメール受信装置の動作を

示したフローチャートである。

【図10】 実施の形態4に係るメール送信装置の機能構成図を示す図である。

【図11】 電子署名情報ファイルを示した図である。

【図12】 実施の形態4に係るメール送信装置の動作を示したフローチャートである。

【図13】 実施の形態5に係るメール受信装置の機能構成図を示す図である。

【図14】 署名検証情報ファイルを示した図である。

【図15】 実施の形態5に係るメール受信装置の動作を示したフローチャートである。

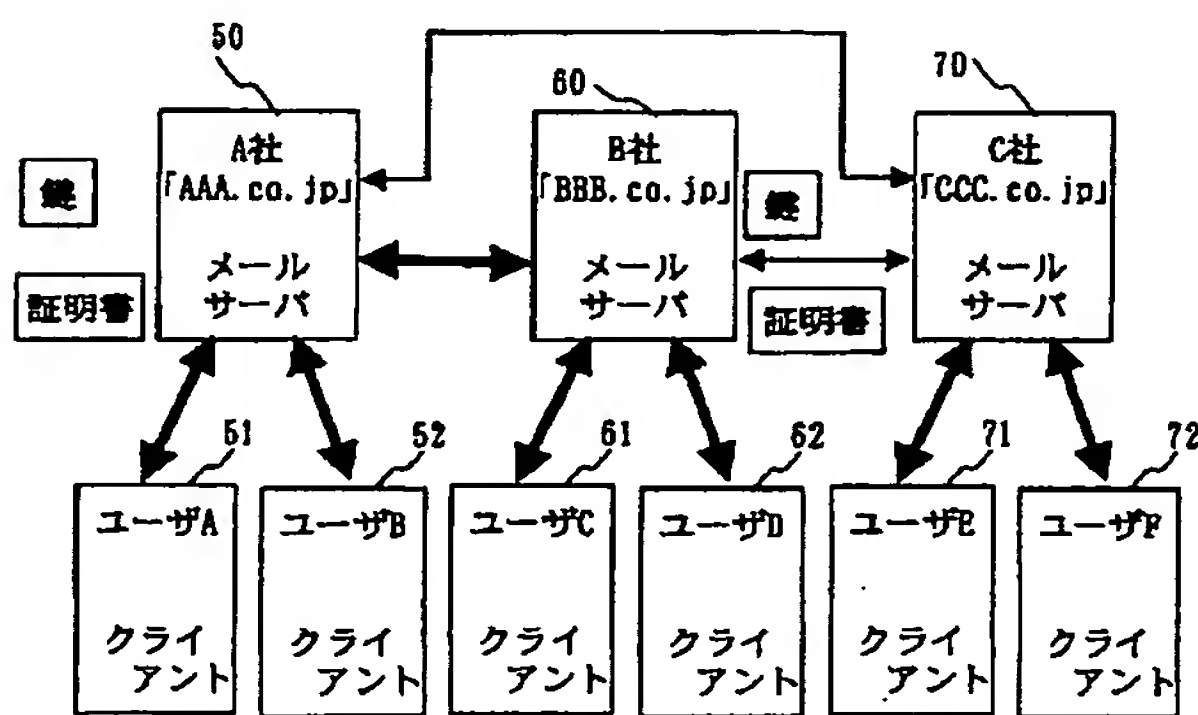
【図16】 従来の技術を説明した簡単な構成図である。

【符号の説明】

1 メール入力部、2 暗号化情報ファイル記憶部（ドメイン名記憶部の一例）、3 認証書データベース、4

メール暗号化部、5 メール送信部、6 暗号化情報ファイル、7 メール受信部、8 復号情報ファイル記憶部（ドメイン名記憶部の一例）、9 秘密鍵記憶部、10 メール復号部、11 メール蓄積部、12 メール出力部、13 復号情報ファイル、14 電子署名情報ファイル記憶部（ドメイン名記憶部の一例）、15 秘密鍵記憶部、16 電子署名部、17 電子署名情報ファイル、18 署名検証情報ファイル記憶部（ドメイン名記憶部の一例）、19 認証書データベース、20 署名検証部、21 署名検証情報ファイル、50 A社のメールサーバ、51、52 A社のクライアントコンピュータ、60 B社のメールサーバ、61、62 B社のクライアントコンピュータ、70 C社のメールサーバ、71、72 C社のクライアントコンピュータ。

【図1】

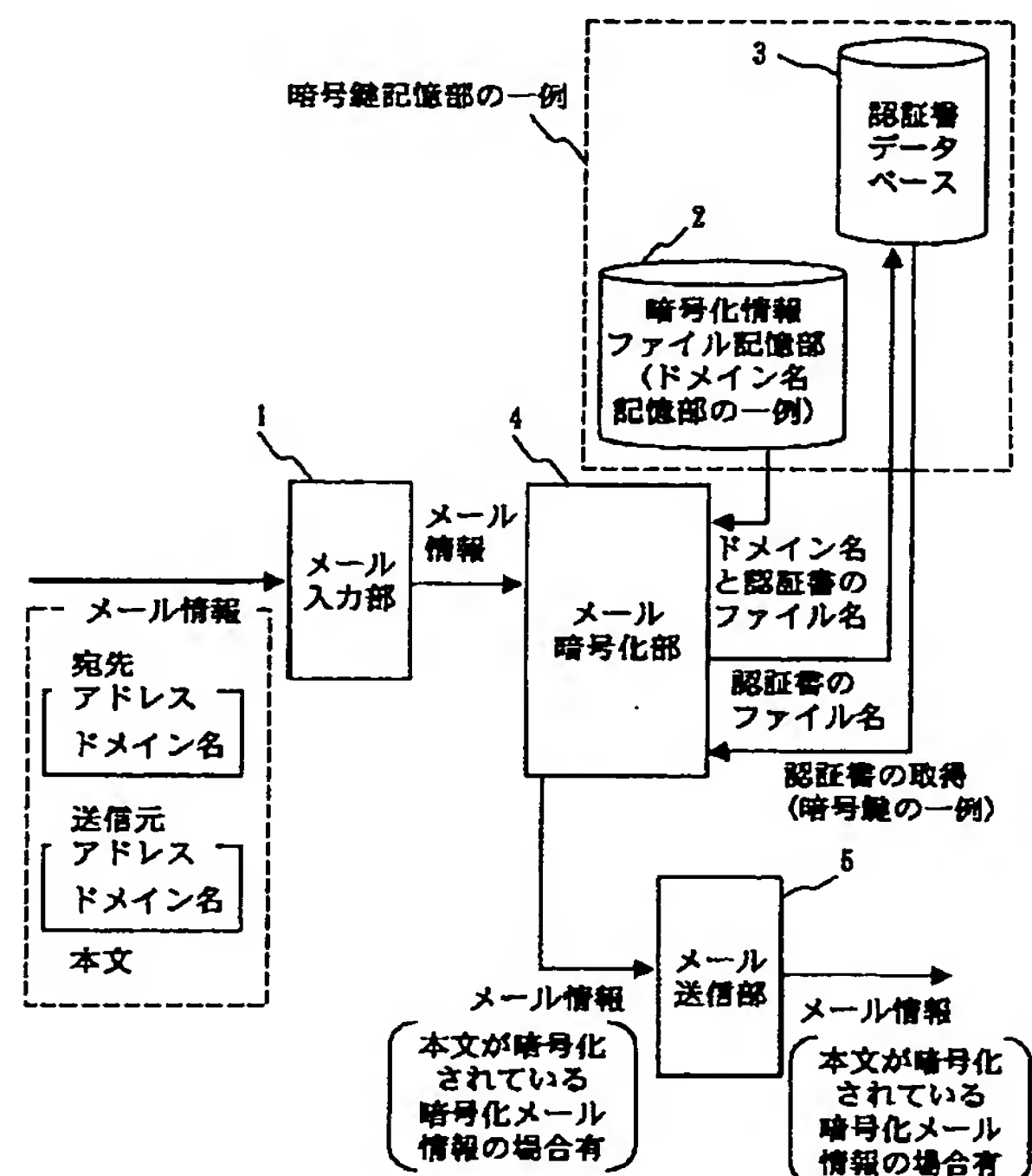


【図3】

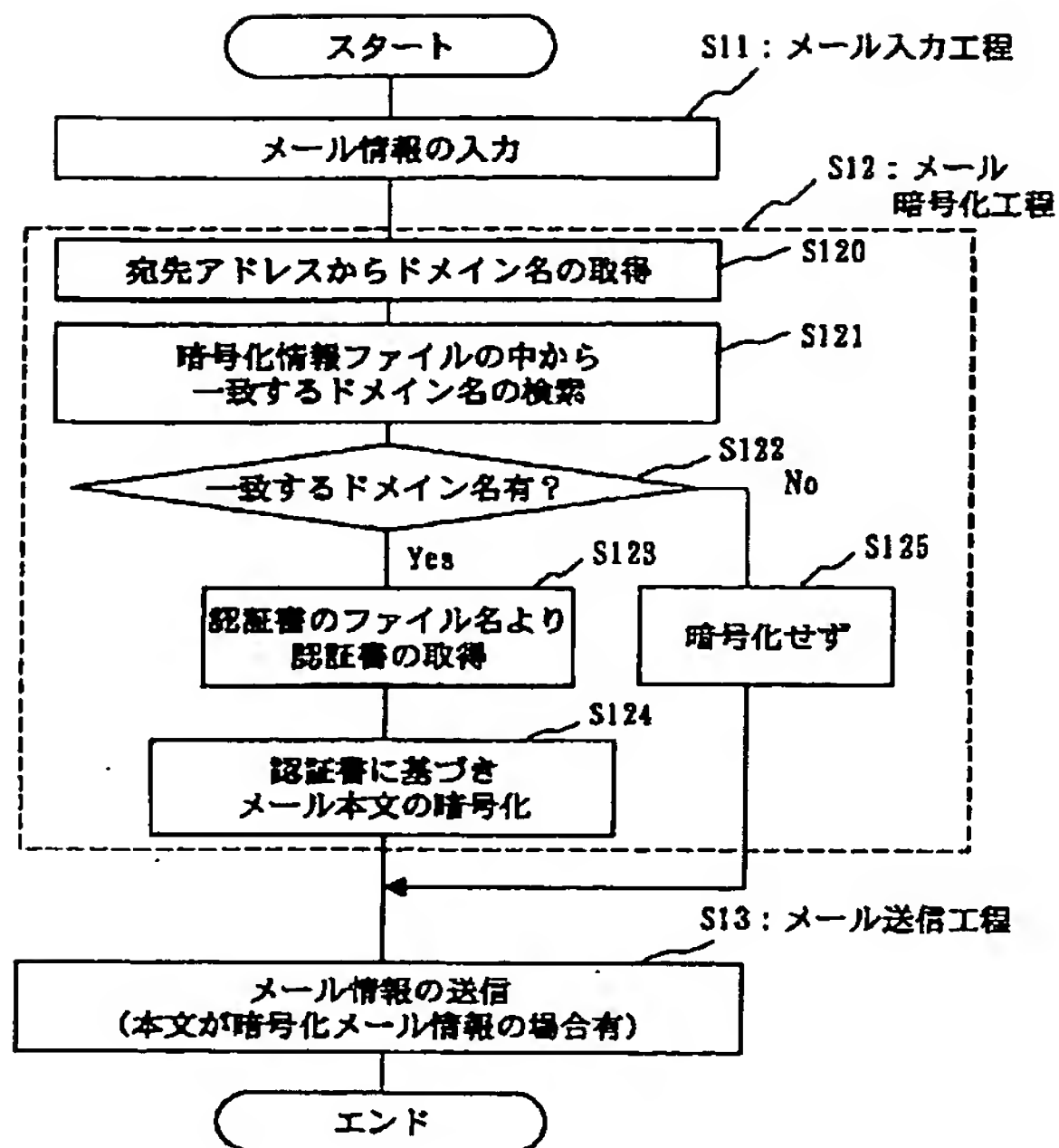
8:暗号化情報ファイル

宛先アドレスのドメイン名	暗号化情報
@BBB.co.jp	認証書のファイル名又は発行者名とシリアル番号 「certification BBB」
@XYZ.co.jp	「certification XYZ」
⋮	⋮

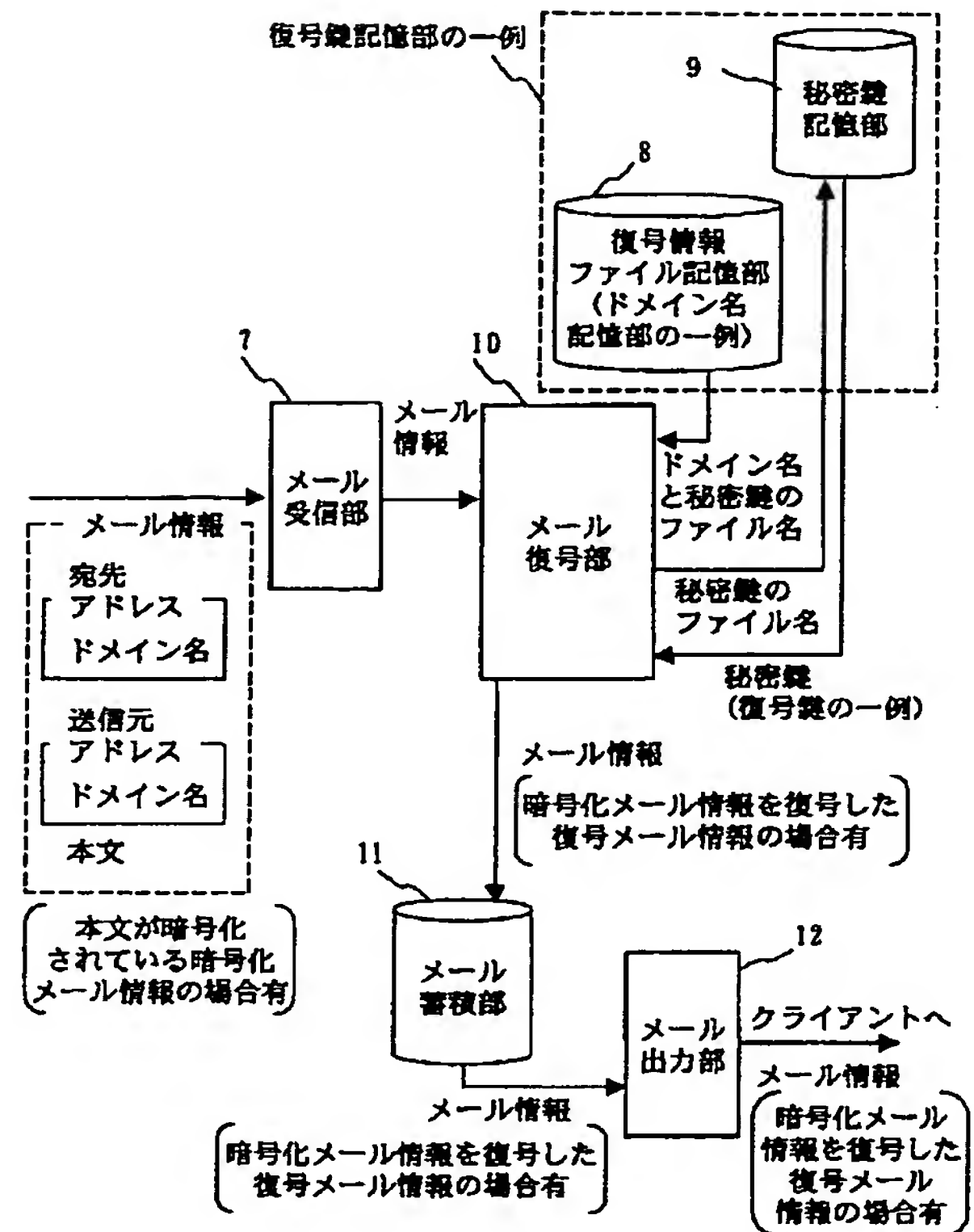
【図2】



【図4】



【図5】



【図6】

13: 復号情報ファイル

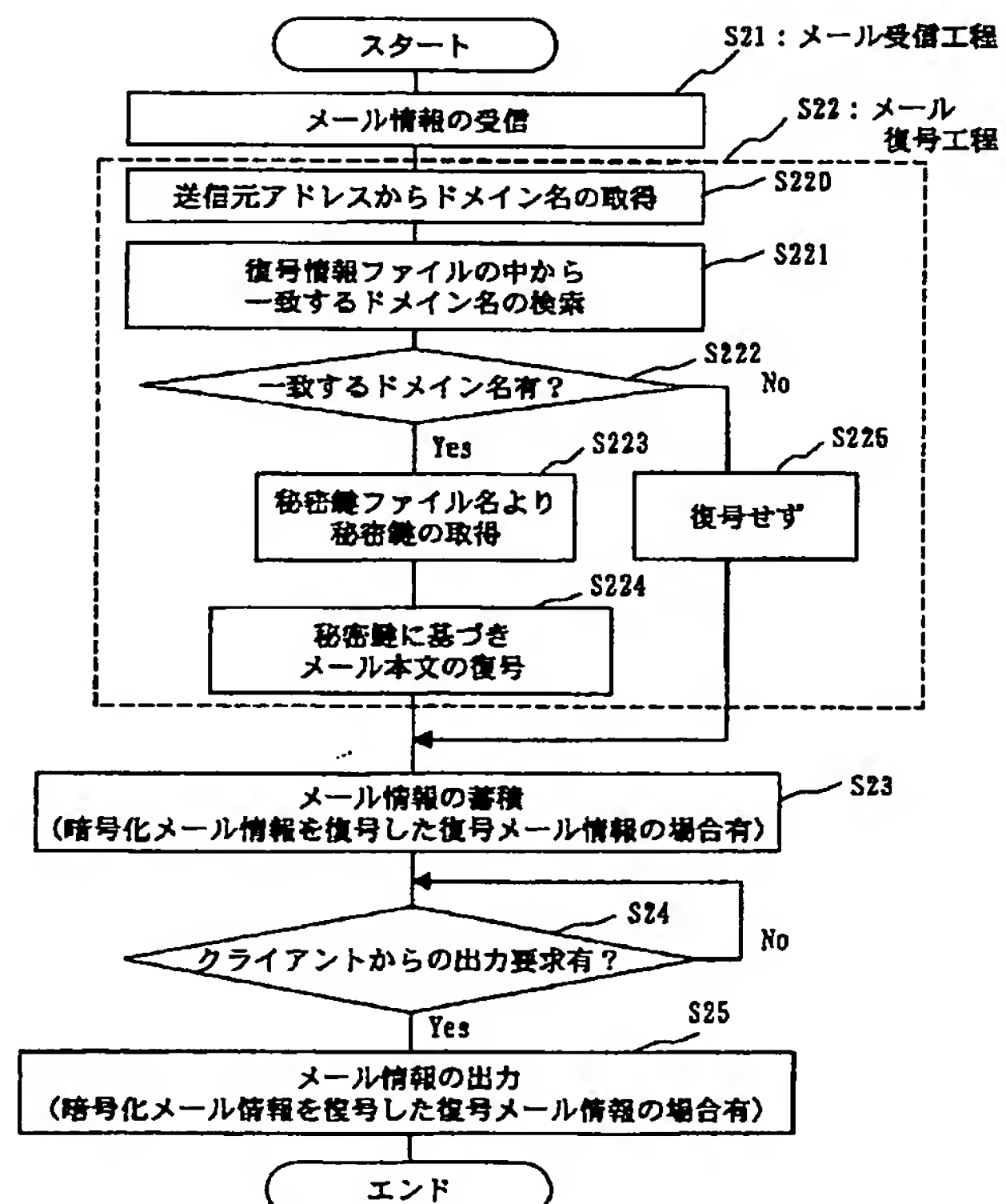
送信元アドレスのドメイン名	復号情報
@YYY.co.jp	秘密鍵1のファイル名 「secret 1」
@SYZ.co.jp	
⋮	

【図11】

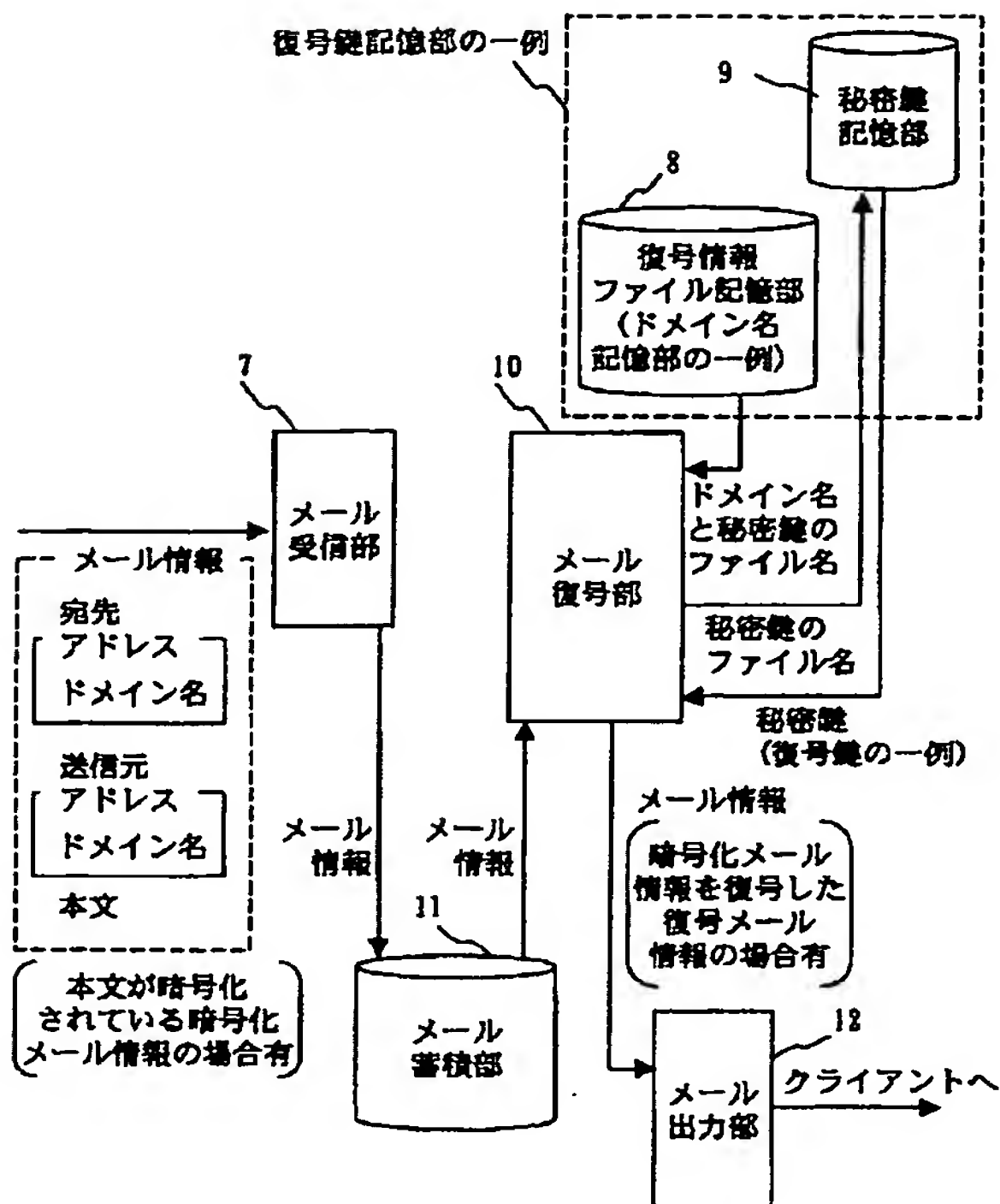
17: 電子署名情報ファイル

宛先アドレスのドメイン名	電子署名情報
@ZZZ.co.jp	秘密鍵2のファイル名 「secret 2」
@ASG.co.jp	
⋮	

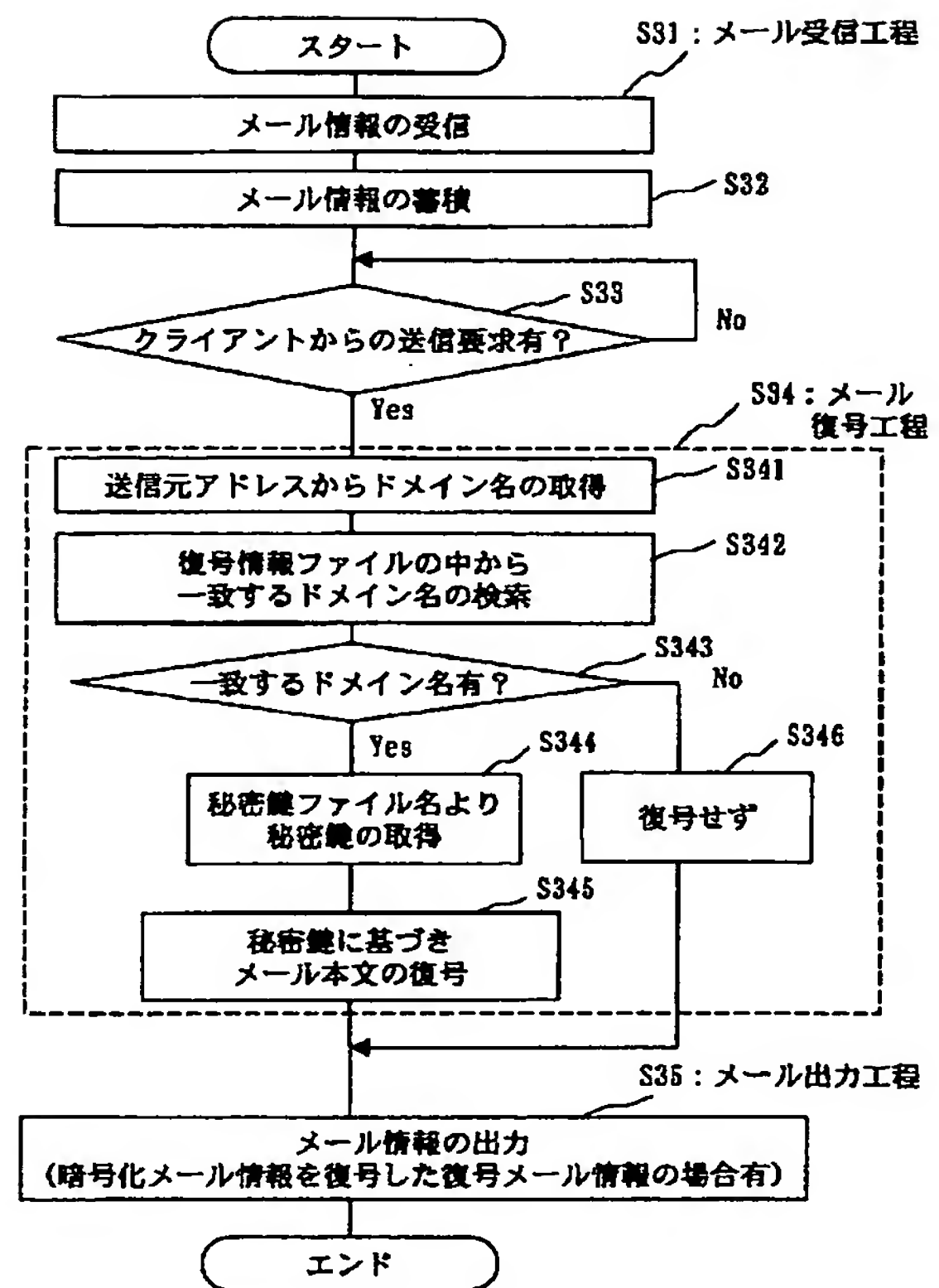
【図7】



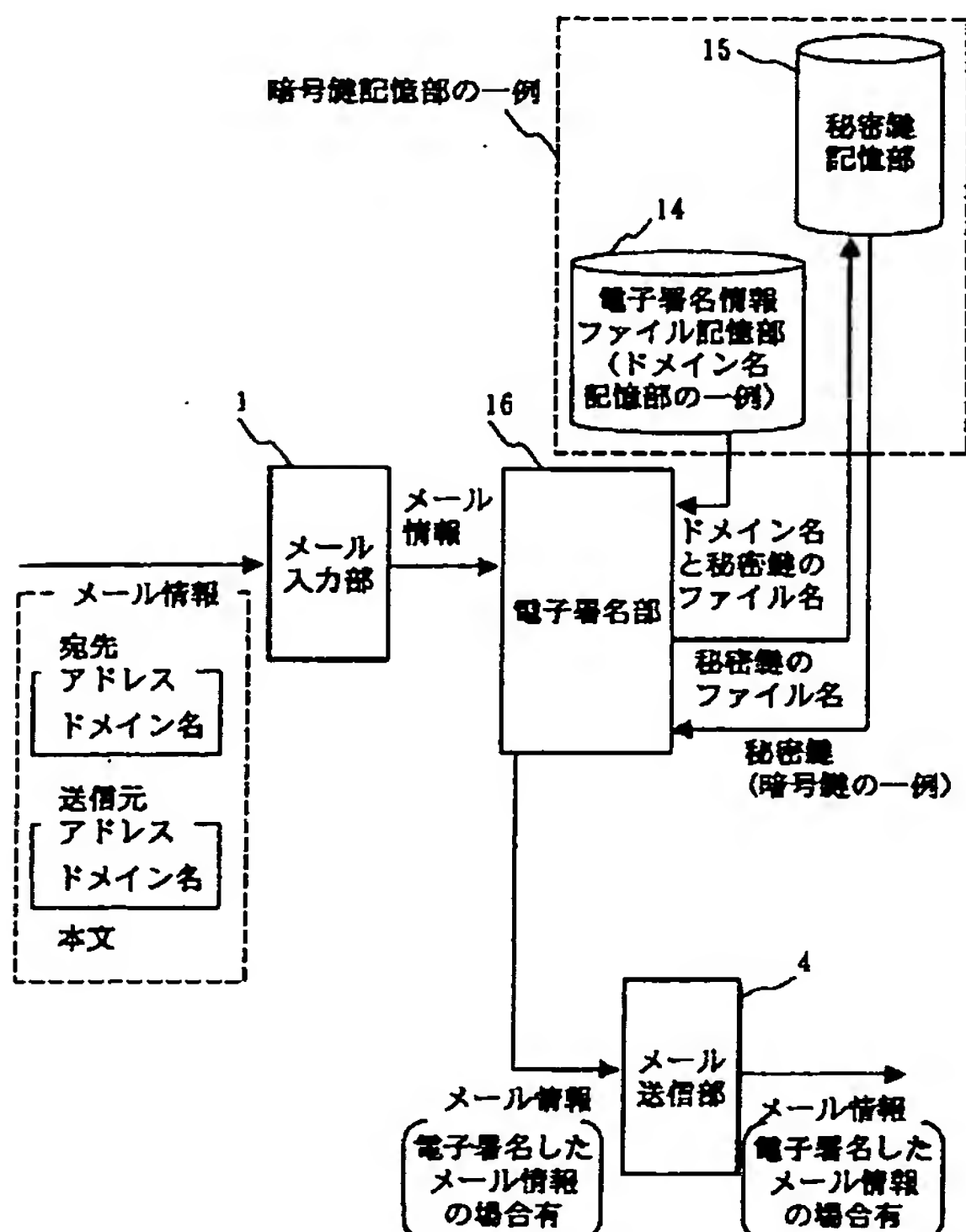
【図 8】



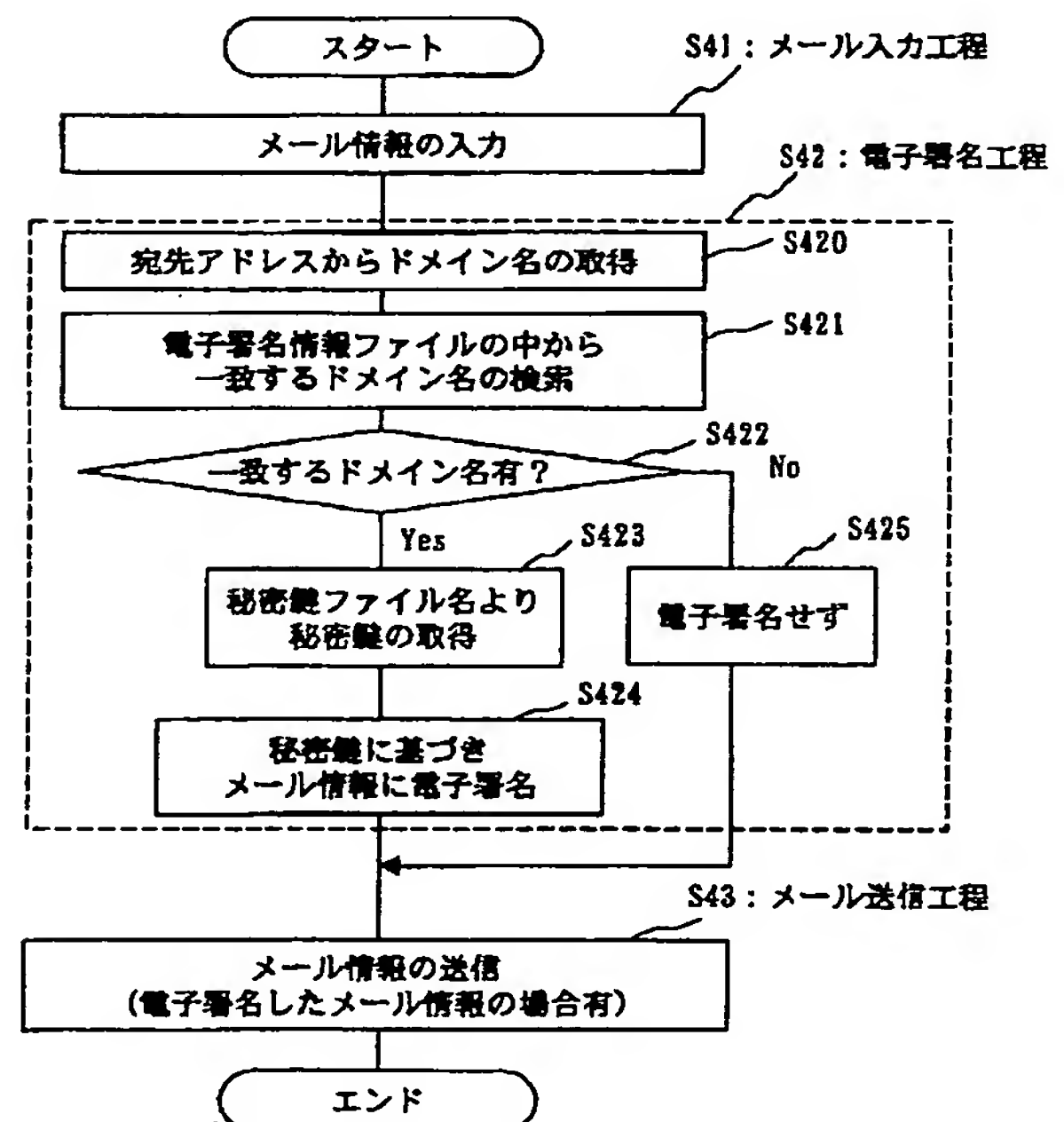
【図 9】



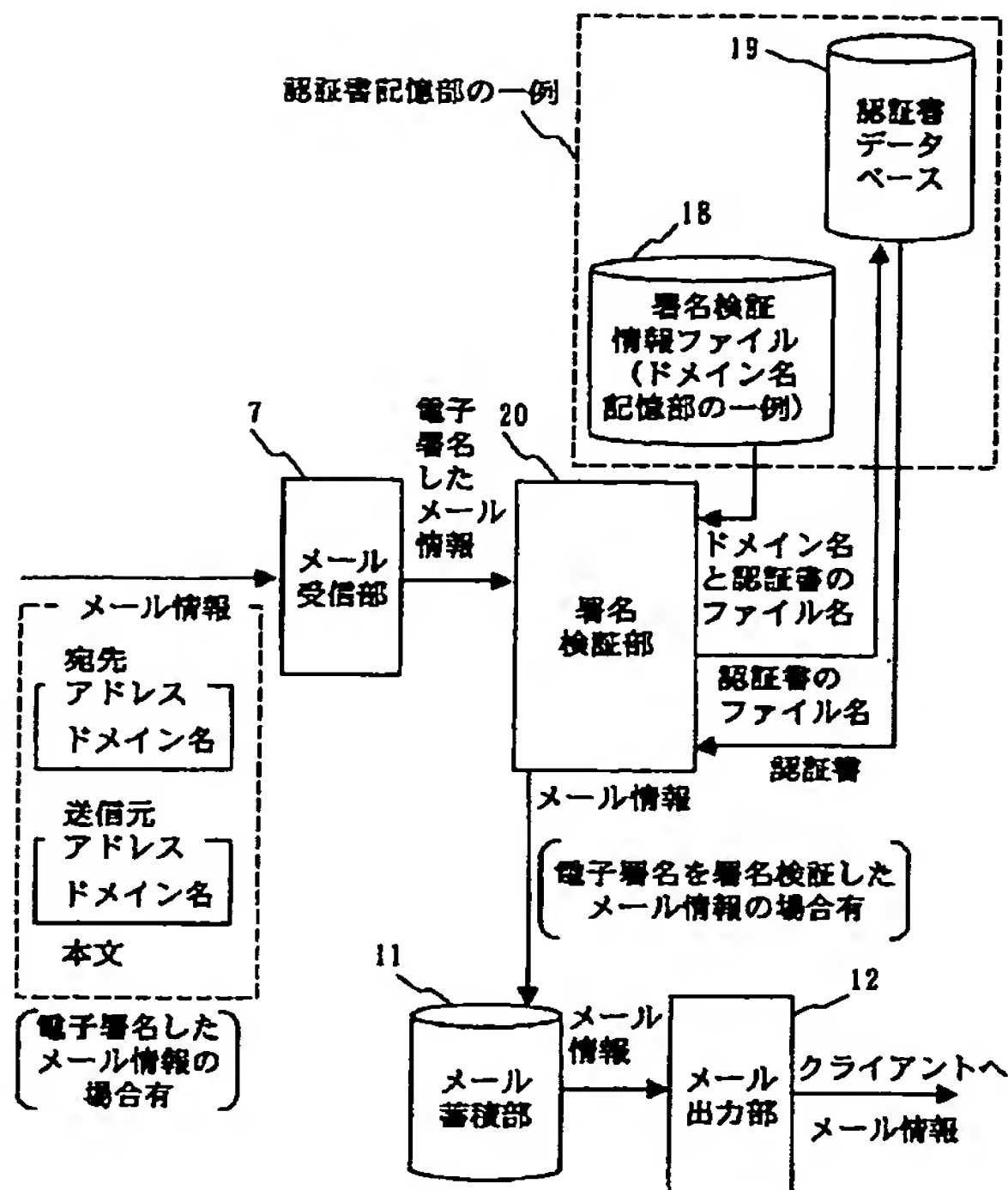
【図 10】



【図 12】



【図 13】

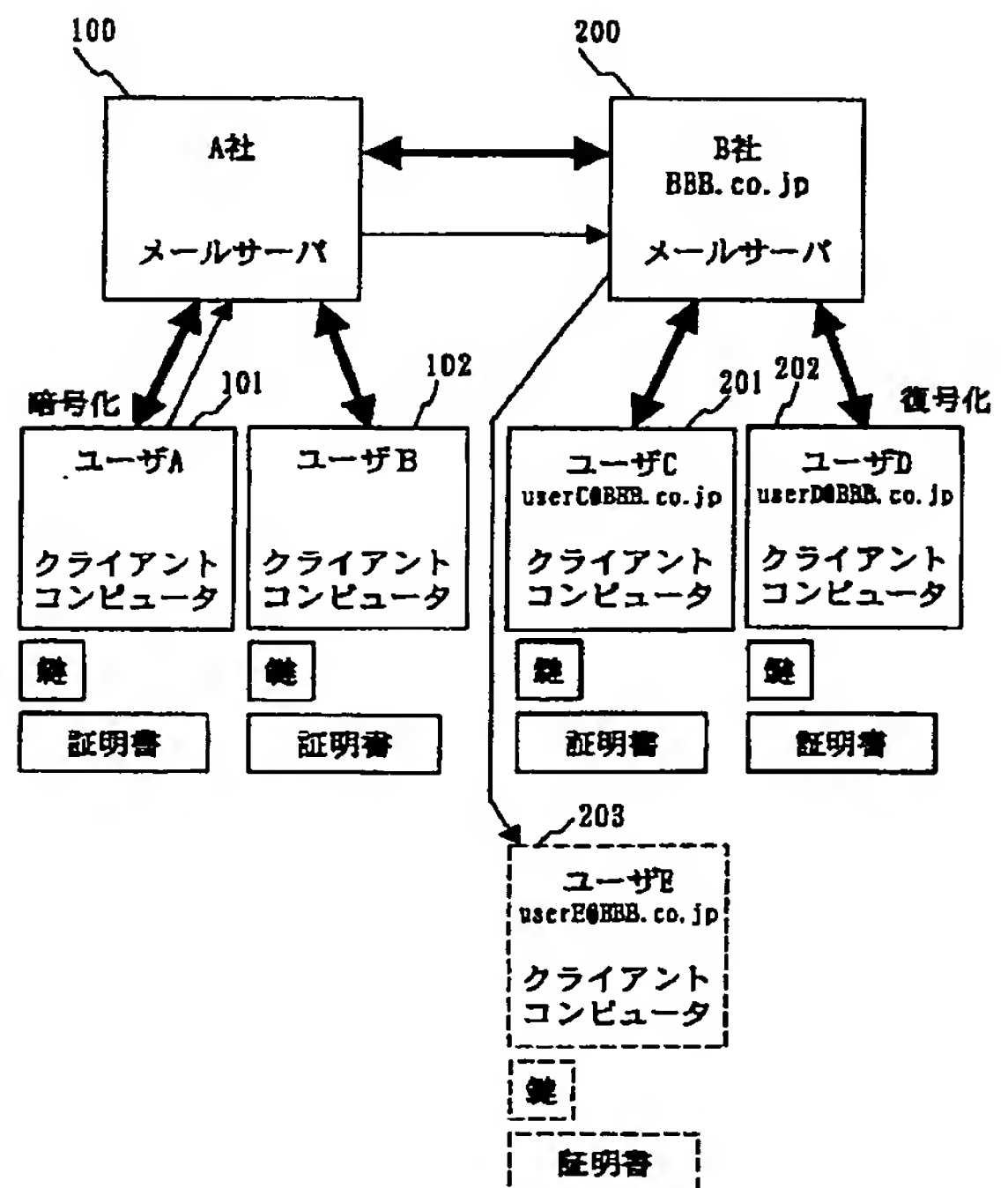


【図 14】

21: 署名検証情報ファイル

送信元アドレスの ドメイン名	署名検証情報
@XYZ.co.jp	認証書のファイル名 「sign XYZ」
@ABS.co.jp	「sign ABS」
⋮	⋮

【図 16】



【図 15】

